

A Note on l -Class Groups of Certain Algebraic Number Fields

NORIKATA NAKAGOSHI

Department of Mathematics, Toyama University, Gofuku 3190, Toyama, Japan

Communicated by Y. Kawada

Received April 20, 1982; revised October 5, 1983

The structure of ideal class groups of number fields is investigated in the following three cases: (i) Abelian extensions of number fields whose Galois groups are of type (p, p) ; (ii) non-Galois extensions $Q(\sqrt[p]{d_0}, \sqrt[p]{d_1})$ of degree p^2 over Q ; (iii) dihedral extensions of degree 2^{n+1} over Q . It is shown that it is possible to obtain class number relations by group-theoretic methods. Subgroups of ideal class groups whose orders are prime to the extension degree are considered. © 1984 Academic Press, Inc.

The subject of this note is the investigation of class number relations and the structure of ideal class groups of certain algebraic number fields. We shall show that it is possible to obtain class number relations by group-theoretic methods from the structure of ideal class groups.

For any algebraic number field K of finite degree over the field Q of rationals we denote by $C_K = I_K/P_K$ the ideal class group of K where I_K is the group of ideals and P_K is the group of principal ideals of K . Then $C_K = \prod_l C_K(l)$ (direct) where $C_K(l)$ is the Sylow l -subgroup of C_K and l ranges over all rational prime numbers.

In this note we consider the structure of $C_K(l)$ and describe class number relations in the following three cases:

- (i) K/k is an Abelian extension of a number field k whose Galois group is of type (p, p) , p is a prime number and $l \neq p$;
- (ii) $K = Q(\sqrt[p]{d_0}, \sqrt[p]{d_1})$ is a non-Galois extension of degree p^2 over Q where p is an odd prime number and $l \neq p$;
- (iii) K is a dihedral extension of degree 2^{n+1} over Q and $l \neq 2$.

We mention here that Brauer [2] and Kuroda [8] formulated analytically class number relations for relatively Galois extensions. Walter [13] and [14] refined Brauer's and Kuroda's results. Shimura [12] described class number relations of dihedral extensions of degree $4n$ ($n > 1$) using the L -function and

properties of CM-fields. On the other hand, class number relations were obtained by purely algebraic and arithmetical methods in two cases: (a) bibyclic biquadratic extensions over Q (Kubota [7]); (b) dihedral extensions of degree $2l$ over Q (Halter-Koch [6]).

Fröhlich [4] obtained class number relations of certain subgroups of the factor group $I_K/P_K I_k$ for an Abelian extension K/k of prime power degree. Cornell-Rosen [3], Fröhlich [4] and Ohta [9] investigated the structure of ideal class groups under certain conditions. We shall show class number relations from the structure of ideal class groups.

In this note we will denote by $|A|$ the order of any finite group A .

THEOREM 1 (cf. Ohta [9]). *Let K/k be an Abelian extension of a number field k whose Galois group is of type (p, p) , p is a prime number. Let k_0, k_1, \dots, k_p be cyclic subfields of K of degree p over k .*

If l is a prime number and $l \neq p$, then

$$C_K(l) = \prod_{n=0}^p C_{k_n}(l), \quad |C_K(l)| = \prod_{n=0}^p |C_{k_n}(l)| / |C_k(l)|^p. \quad (1)$$

Proof. Let G and $G_n = \langle \sigma_n \rangle$ ($n = 0, 1, \dots, p$) be the Galois group of K over k and Galois groups of K over k_n , respectively, where σ_n is a generator of G_n for each n . Let us form the sums

$$\bar{G} = \sum_{\sigma \in G} \sigma, \quad \bar{G}_n = \sum_{s=0}^{p-1} \sigma_n^s$$

of elements of G and G_n in the group ring $Z[G]$, respectively, where Z is the ring of rational integers. Then we have

$$\sum_{n=0}^p \bar{G}_n = \bar{G} + p \cdot 1.$$

Let $j: C_k \rightarrow C_K$ and $j_n: C_{k_n} \rightarrow C_K$ be the homomorphisms of the class groups of k and k_n to that of K induced by extension of ideals, respectively ($n = 0, 1, \dots, p$). Let l be a prime number and $l \neq p$. If c_n is an element of $C_{k_n}(l)$ and $j_n(c_n) = 1$, then $N_{K/k_n}(j_n(c_n)) = c_n^p = 1$ and so $c_n = 1$ in C_{k_n} , where N_{K/k_n} is the norm map. Consequently we have $j_n(C_{k_n}(l)) \cong C_{k_n}(l)$ for each $n = 0, 1, \dots, p$. Similarly we have $j(C_k(l)) \cong C_k(l)$. Thus we may consider $C_{k_n}(l)$ and $C_k(l)$ as subgroups of $C_K(l)$.

We have for any x of C_K

$$x^p = \prod_{n=0}^p x^{\bar{G}_n} / x^{\bar{G}}.$$

Since $C_K(l) = C_K(l)^p = \{x^p \mid x \in C_K(l)\}$, it follows that

$$C_K(l) = \prod_{n=0}^p j_n(C_{k_n}(l)) = \prod_{n=0}^p C_{k_n}(l).$$

If y is an element of $j_0(C_{k_0}(l)) \cap j_1(C_{k_1}(l))$, then $y^{\sigma_0} = y^{\sigma_1} = y$ and also $y^p = y^{\bar{\sigma}_0} = y^{\bar{\sigma}_1}$ which is an element of $j(C_k(l)) = C_k(l)$. Since $j_0(C_{k_0}(l)) \cap j_1(C_{k_1}(l)) = \{y^p \mid y \in j_0(C_{k_0}(l)) \cap j_1(C_{k_1}(l))\}$, we have $j_0(C_{k_0}(l)) \cap j_1(C_{k_1}(l)) = j(C_k(l)) = C_k(l)$.

If z is an element of $j_2(C_{k_2}(l)) \cap (j_0(C_{k_0}(l)) \cdot j_1(C_{k_1}(l)))$, then $z = z_0 z_1$ with z_0 in $j_0(C_{k_0}(l))$ and z_1 in $j_1(C_{k_1}(l))$. We have $z^p = z^{\bar{\sigma}_2} = z_0^{\bar{\sigma}_2} z_1^{\bar{\sigma}_2}$ which is an element of $j(C_k(l)) = C_k(l)$. Hence we have $j_2(C_{k_2}(l)) \cap (j_0(C_{k_0}(l)) \cdot j_1(C_{k_1}(l))) = C_k(l)$. It then follows inductively that

$$j_n(C_{k_n}(l)) \cap \prod_{r=0}^{n-1} j_r(C_{k_r}(l)) = C_k(l) \quad (2)$$

for $n = 1, \dots, p$. Thus we have

$$\begin{aligned} |C_K(l)| &= \left| \prod_{n=0}^p j_n(C_{k_n}(l)) \right| \\ &= \left| \prod_{n=0}^{p-1} j_n(C_{k_n}(l)) \right| |C_{k_p}(l)| |C_k(l)| = \dots \\ &= \prod_{n=0}^p |C_{k_n}(l)| |C_k(l)|^p. \end{aligned}$$

We denote by $\sqrt[p]{d}$ the real p th root of d if p is an odd prime number and d is real.

THEOREM 2. *Let p be an odd prime number. Let d_0, d_1 be positive p th power free rational integers ($\neq 1$) such that $k_0 = Q(\sqrt[p]{d_0})$ and $k_1 = Q(\sqrt[p]{d_1})$ are distinct pure fields of degree p over Q . We put $k_n = Q(\sqrt[p]{d_0^{n-1} d_1})$ for $n = 2, \dots, p$ and $K = Q(\sqrt[p]{d_0}, \sqrt[p]{d_1})$.*

If l is a prime number and $l \neq p$, then

$$C_K(l) = \prod_{n=0}^p C_{k_n}(l) \quad (\text{direct}), \quad (3)$$

$$|C_K(l)| = \prod_{n=0}^p |C_{k_n}(l)|. \quad (3')$$

In order to prove Theorem 2 we need the following lemma which was produced by the referee:

LEMMA 3. Let p be an odd prime number and ζ be a primitive p th root of unity. We put $L_n = k_n(\zeta)$ for $n = 0, 1, \dots, p$ and $L = K(\zeta)$ where k_n and K are defined by Theorem 2.

Let \bar{K} and \bar{k}_n be Hilbert class fields of K and k_n for $n = 0, 1, \dots, p$, respectively. Then we have

$$L_n \cap \bar{k}_n = k_n \quad (n = 0, 1, \dots, p)$$

and

$$L \cap \bar{K} = K.$$

Proof. According to [1] or [15] there are two possible factorizations of the prime p in the field k_n . Either

$$(p) = \mathfrak{p}_1^p$$

with degree 1 or

$$(p) = \mathfrak{p}_1 \mathfrak{p}_2^{p-1}$$

with both factors of degree 1. We shall say that k_n is of Type 1 or Type 2 according as p has the first or the second factorization in k_n . If k_n is of Type 1, then \mathfrak{p} is totally ramified in L_n and so $L_n \cap \bar{k}_n = k_n$. If k_n is of Type 2, then \mathfrak{p}_1 is totally ramified in L_n and \mathfrak{p}_2 splits completely in L_n , since p is totally ramified in $Q(\zeta)$ and $(L_n : Q) = p(p-1)$. Thus $L_n \cap \bar{k}_n = k_n$.

The proof that $L \cap \bar{K} = K$ will be divided into three cases:

Case 1. Each k_n ($n = 0, 1, \dots, p$) is of Type 1.

Case 2. K contains a subfield k_1 of Type 1 and a subfield k_2 of Type 2.

Case 3. Each k_n ($n = 0, 1, \dots, p$) is of Type 2.

Case 1. Here p ramifies totally in each field L_n . Since L/L_n is cyclic of degree p , the prime factor of p in L_n must ramify totally in L or not ramify at all in L . Assume the latter and let k be the inertial field over Q of any prime divisor of p in L . Then k is an extension of Q of degree p contained in L and so must be conjugate to some field k_n . This contradicts the fact that p ramifies totally in k_n . Hence it follows that $L \cap \bar{K} = K$.

Case 2. Here the factorization of p in L_2 has the form

$$(p) = (\mathfrak{p}'_1 \mathfrak{p}'_2 \cdots \mathfrak{p}'_g)^{p-1}.$$

If the factorization of p in L has the form

$$(p) = (\mathfrak{P}'_1 \mathfrak{P}'_2 \cdots \mathfrak{P}'_g)^e,$$

then both p and $p-1$ must divide e , and $g \geq p$. Since $eg \leq p^2(p-1)$ it follows that $e = p(p-1)$ and $g = p$. Since k_1 is of Type 1 and k_2 is of Type 2, it is easily seen that $(p) = \mathfrak{P}_1^{p(p-1)} \mathfrak{P}_2^p$ in K where \mathfrak{P}_1 and \mathfrak{P}_2 are prime ideals of degree 1. Thus \mathfrak{P}_2 ramifies totally in L and so $L \cap \bar{K} = K$.

Case 3. Here $(p) = (p')^{p-1}$ in $Q(\zeta)$ and p' splits completely in both L_1 and L_2 and hence in the composite field $L = L_1 L_2$. Thus p has p^2 distinct prime ideal factors in L , each of degree 1 and ramification index $p-1$ over Q . Thus, if k is the inertial field over Q of any prime divisor of p in L , then $(k:Q) = p^2$ and so k must be one of the p^2 conjugates of the field K . Hence L/K is a totally ramified extension and so $L \cap \bar{K} = K$.

Proof of Theorem 2. We use the notation of Lemma 3 and put $\Omega = Q(\zeta)$. It is clear that L/Ω is an Abelian extension of type (p, p) . Let l be a prime number and $l \neq p$. Then we may consider $C_{L_n}(l)$ as subgroups of $C_L(l)$ and $C_{k_n}(l)$ as subgroups of $C_K(l)$. It follows from (1) that

$$C_L(l) = \prod_{n=0}^p C_{L_n}(l).$$

We then have

$$N_{L/K}(C_L(l)) = N_{L/K} \left(\prod_{n=0}^p C_{L_n}(l) \right) = \prod_{n=0}^p N_{L_n/k_n}(C_{L_n}(l))$$

where $N_{L/K}$ is the norm map from L to K and N_{L_n/k_n} are norm maps from L_n to k_n for $n = 0, 1, \dots, p$.

Now it follows that

$$C_L / {}_N C_L \cong N_{L/K} C_L, \quad C_{L_n} / {}_N C_{L_n} \cong N_{L_n/k_n} C_{L_n}$$

where ${}_N C_L$ and ${}_N C_{L_n}$ are kernels of norm maps. From class field theory

$$|N_{L/K} C_L| = |C_K| / (L \cap \bar{K} : K), \quad |N_{L_n/k_n} C_{L_n}| = |C_{k_n}| / (L_n \cap \bar{k}_n : k_n)$$

for $n = 0, 1, \dots, p$. From Lemma 3 the norm map $N_{L/K} : C_L \rightarrow C_K$ and the norm maps $N_{L_n/k_n} : C_{L_n} \rightarrow C_{k_n}$ are surjective for $n = 0, 1, \dots, p$.

By (2) we have $C_{L_n}(l) \cap (C_{L_0}(l) \cdots C_{L_{n-1}}(l)) = C_{\Omega}(l)$ which shows $C_{k_n}(l) \cap (C_{k_0}(l) \cdots C_{k_{n-1}}(l)) = 1$ for $n = 1, \dots, p$ by the norm map. Thus we have (3) and (3').

In case of $p = 3$, Parry [11] already obtained the class number relation for $Q(\sqrt[3]{d_0}, \sqrt[3]{d_1})$ using the analytic results of Kuroda [8]. In this note we do not deal with the 3-component of the class number of $Q(\sqrt[3]{d_0}, \sqrt[3]{d_1})$ which is determined by [11].

THEOREM 4. *Let K/Q be a dihedral extension of degree 2^{n+1} ($n \geq 2$). Let $\text{Gal}(K/Q) = \langle \sigma, \tau \mid \sigma^{2^n} = \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} \rangle$ be the Galois group of K over Q . Let $K_1^{(v)}$ and $K_2^{(v)}$ be the fixed fields to $\langle \tau, \sigma^{2^v} \rangle$ and $\langle \sigma\tau, \sigma^{2^v} \rangle$, respectively ($v = 1, \dots, n$). Let $K_0^{(v)}$ be the fixed fields to $\langle \sigma^{2^v} \rangle$ ($v = 0, 1, \dots, n-1$).*

If l is an odd prime number, then we have

$$\frac{|C_{K_1^{(v)}}(l)|}{|C_{K_1^{(v-1)}}(l)|} = \frac{|C_{K_2^{(v)}}(l)|}{|C_{K_2^{(v-1)}}(l)|} \quad (4)$$

for $v = 2, \dots, n$ and

$$|C_K(l)| = |C_{K_0^{(0)}}(l)| |C_{K_1^{(n)}}(l)| |C_{K_2^{(n)}}(l)|. \quad (5)$$

If $n = 2$, Parry [10] determined the class number relation using the analytic results. The 2-component $|C_K(2)|$ is also obtained by [10] for $n = 2$.

In order to prove Theorem 4 we need the following lemma which can be obtained from (1):

LEMMA 5. *Let (K, k_1, k_2) be a set of algebraic number fields satisfying the following conditions:*

- (i) K/k_1 and K/k_2 are Abelian extensions of type $(2, 2)$;
- (ii) K_i, K'_i and $K_0 = k_1 k_2$ are quadratic subfields of K over k_i for each $i = 1, 2$;
- (iii) K_i and K'_i are conjugate over Q for each $i = 1, 2$.

If l is an odd prime number, then

$$|C_K(l)| = \begin{cases} |C_{K_0}(l)| |C_{K_1}(l)|^2 / |C_{k_1}(l)|^2 \\ |C_{K_0}(l)| |C_{K_2}(l)|^2 / |C_{k_2}(l)|^2 \end{cases}$$

and hence

$$\frac{|C_{K_1}(l)|}{|C_{k_1}(l)|} = \frac{|C_{K_2}(l)|}{|C_{k_2}(l)|}.$$

Proof of Theorem 4. We note that $\langle \sigma^{2^\lambda} \tau \rangle$ are conjugate to $\langle \tau \rangle$ and $\langle \sigma^{2^{\lambda+1}} \tau \rangle$ are conjugate to $\langle \sigma \tau \rangle$ for $\lambda = 0, 1, \dots, 2^{n-1} - 1$ (cf. [5]). For each v ($1 \leq v \leq n-1$) $\langle \sigma^{2^{v+1}}, \sigma^{2^\lambda} \tau \rangle$ are conjugate to $\langle \sigma^{2^{v+1}}, \tau \rangle$ and $\langle \sigma^{2^{v+1}}, \sigma^{2^{\lambda+1}} \tau \rangle$ are conjugate to $\langle \sigma^{2^{v+1}}, \sigma \tau \rangle$ for $\lambda = 0, 1, \dots, 2^v - 1$. Then the sets $(K, K_1^{(n-1)}, K_2^{(n-1)}, (K_0^{(n-1)}, K_1^{(n-2)}, K_2^{(n-2)}), \dots, (K_0^{(2)}, K_1^{(1)}, K_2^{(1)}))$ satisfy the conditions of Lemma 5. Hence (4) is immediately obtained.

Finally for $i = 1, 2$ we have

$$\begin{aligned}
 |C_K(I)| &= |C_{K_1^{(n)}}(I)|^2 |C_{K_0^{(n-1)}}(I)| / |C_{K_1^{(n-1)}}(I)|^2 \\
 &= |C_{K_1^{(n)}}(I)|^2 |C_{K_0^{(n-2)}}(I)| / |C_{K_1^{(n-2)}}(I)|^2 \\
 &\quad \dots \\
 &= \begin{cases} |C_{K_1^{(n)}}(I)|^2 \frac{1}{|C_{K_1^{(1)}}(I)|} |C_{K_0^{(0)}}(I)| |C_{K_2^{(1)}}(I)| \\ |C_{K_2^{(n)}}(I)|^2 \frac{1}{|C_{K_2^{(1)}}(I)|} |C_{K_0^{(0)}}(I)| |C_{K_1^{(1)}}(I)|. \end{cases}
 \end{aligned}$$

It then follows that $|C_K(I)|^2 = (|C_{K_0^{(0)}}(I)| |C_{K_1^{(n)}}(I)| |C_{K_2^{(n)}}(I)|)^2$ which shows (5).

ACKNOWLEDGMENT

I am grateful to the Referee for his comments.

REFERENCES

1. W. E. H. BERWICK "Integral Bases," Cambridge Tracts in Mathematics and Mathematical Physics No. 22, Stochert-Hafner, New York, 1964.
2. R. BRAUER, Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers, *Math. Nachr.* **4** (1950/51), 158–174.
3. G. CORNELL AND M. ROSEN, Group-theoretic constraints on the structure of the class groups, *J. Number Theory* **13** (1981), 1–11.
4. A. FRÖHLICH, On the class group of relatively Abelian fields, *Quart. J. Math. Oxford* (2) **3** (1952), 98–106.
5. F. HALTER-KOCH, Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Diedergruppe, *J. Number Theory* **3** (1971), 412–443.
6. F. HALTER-KOCH, Einheiten und Divisorenklassen in Galoisschen algebraischen Zahlkörpern mit Diedergruppe der Ordnung $2l$ für eine ungerade Primzahl l , *Acta Arith.* **33** (1977), 353–364.
7. T. KUBOTA, Über den bzyklischen biquadratischen Zahlkörper, *Nagoya Math. J.* **10** (1956), 65–85.
8. S. KURODA, Über die Klassenzahlen algebraischer Zahlkörper, *Nagoya Math. J.* **1** (1950), 1–10.
9. K. OHTA, On the p -class group of a Galois number field and its subfields, *J. Math. Soc. Japan* **30** (1978), 763–770.
10. C. J. PARRY, Pure quartic number fields whose class numbers are even, *J. Reine Angew. Math.* **272** (1975), 102–112.
11. C. J. PARRY, Class number formulae for bicubic fields, *Illinois J. Math.* **21** (1977), 148–163.

12. G. SHIMURA, On Abelian varieties with complex multiplication, *Proc. London Math. Soc.* (3) **34** (1977), 65–86.
13. C. D. WALTER, Brauer's class number relation, *Acta Arith.* **35** (1979), 33–40.
14. C. D. WALTER, Kuroda's class number relation, *Acta Arith.* **35** (1979), 41–51.
15. J. WESTLUND, On the fundamental number of the algebraic number field $k(\sqrt[p]{m})$, *Trans. Amer. Soc.* **11** (1920), 338–392.